REMARKS/ARGUMENTS

These remarks are submitted in response to the Office Action of August 19, 2008 (Office Action). As this response is timely filed within the 3-month shortened statutory period, no fee is believed due. However, the Examiner is expressly authorized to charge any deficiencies or credit any overpayments to Deposit Account 50-0951.

Claim Rejections – 35 USC § 103

In the Office Action, Claims 1-18 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Published Patent Application 2003/0217137 to Roese (hereinafter Roese) in view of U.S. Published Patent Application 2003/0115481 to Baird (hereinafter Baird), and in further view of U.S. Published Patent Application 2004/0123150 to Wright, *et al.* (hereinafter Wright) and U.S. Patent 7,140,035 to Karch (hereinafter Karch).

Applicants respectfully disagree with the rejections and thus have not amended the claims to overcome the cited prior art references. Applicants have cancelled Claims 7-19. However, Applicants are not conceding that the cancelled claims fail to present patentable subject matter. The cancellations are solely for the purpose of expediting prosecution. Accordingly, the cancellations should not be interpreted as the surrender of any subject matter, and Applicants expressly reserve the right to present the original version of any of the cancelled claims in any future divisional or continuation applications from the present application.

Certain Aspects Of Applicants' Invention

At this juncture, it may be helpful to reiterate certain aspects of Applicants' invention. One embodiment of the invention, typified by Claim 1, is a method for managing a presentation of sensitive content in non-trusted environments.

The method can include interrogating a list of one or more corporate policies associated with a given user and with a physical device. The policy data can be acquired locally from the physical device or dynamically via access to a corporate network. Each corporate policy prohibits or restricts access to corporate data in a non-trusted environment. The method also can include determining a location of the physical device, and determining whether the user and the physical device is in a trusted or non-trusted environment by comparing the location of the physical device with a list of trusted locations. The list of trusted locations can be embedded within the policy data or stored separately. (See, e.g., Specification, paragraphs [0011] to [0013].)

The method also can include providing access to a subscription-based service, which maintains an organization list comprising individuals and machine identification information. The organization list can identify and indicate that a particular individual or machine listed is associated with a predetermined competitive organization. The method further can include determining that an individual or machine identified on the list associated with the competitive organization is within a predetermined proximity of the physical device. Further according to the method, if it is determined that an individual or machine identified on the list is within a predetermined proximity of the physical device, then an alert can be transmitted to a user via the physical device. (See, e.g., Specification, paragraph [0019].)

Additionally, the method can include enforcing a plurality of rules contained in the policy for managing the presentation of sensitive content. More particularly, the rules can be enforced by blocking a visual presentation or audible presentation of at least one object in portions of the presentation if (1) the physical device is not located in a trusted location, or (2) an individual or a machine identified on the competitive organization list is within a predetermined proximity of the physical device. (See, e.g., Specification, paragraph [0014].)

The Claims Define Over The References

As discussed in the previous response, Roese does not disclose interrogating a list of one or more corporate policies associated with a given user and a physical device, as recited in independent Claim 1 of the instant application. It is noted that user authentication (using password, access card, or fingerprint; see Specification, paragraph [0015], lines 8-15) is different from interrogation of a list of one or more corporate policies to determine the relevant policy that dictates how sensitive content should be displayed in a non-trusted environment. Roese also does not disclose using a subscription-based service to detect individuals or devices associated with a competitive organization and alerting the user when such an individual or device of the competitive organization is within a predetermined proximity of the user's physical device, as recited in independent Claim 1 of the instant application. Roese further does not disclose determining that an individual or machine identified on the list associated with a competitive organization is within a predetermined proximity of the physical device, and in response thereto, transmitting an alert to the physical device, as recited in independent Claim 1 of the instant application. Baird does not make up for the above deficiencies of Roese.

Wright specially addresses the delivery of content (documents as well as applications) from a server to a mobile device. Wright is limited to a mobile device, which contains no "local" content. Rather, it depends on a server to deliver the content (or to limit delivery of the content) via the techniques described. In contrast, the present invention deals with the more common case of content already residing on a device like a laptop with a populated hard drive, containing sensitive documents and not dependent on a remote server for access. Wright, therefore, does not concern the problem solved by the present invention at all.

It is described in paragraph [0078] of Wright that the location detection module 208 determines whether the mobile device is operating in the "work" location network

environment. It is described in paragraph [0080] that the policy for the "software lab" environment allows a mobile device accessing a corporate server to access certain files while a mobile device trying to access the files via the conference room NAP receives a notification that these files cannot be found. It is not clear how these descriptions have anything to do with interrogating a list of one or more corporate policies associated with a given user and a physical device, as recited in independent Claim 1 of the instant application. Wright concerns providing different security policies to be enforced based on a location associated with a network environment in which a mobile device is operating. In contrast, in the present invention the policies are associated with a given user and a physical device, not with a location or a network environment in which the device is located.

Karch describes the application of business rules to limit document access for specific individuals. In contrast, the present invention determines whether an individual or machine associated with a competitive organization is located within a predetermined proximity of the physical device, and in response thereto, transmits an alert to the physical device. It is noted that in the present invention the determination depends on the location of the individual, not the identity of the individual.

Further, the present invention describes the invocation of a subscription-based service to determine the location, for example, using GPS. This is not disclosed by any of the cited references.

Accordingly, the cited references, alone or in combination, fail to disclose or suggest each and every element of Claim 1, as amended. Applicants therefore respectfully submit that amended Claim 1 defines over the prior art. Furthermore, as each of the remaining claims depends from Claim 1 while reciting additional features, Applicants further respectfully submit that the remaining claims likewise define over the prior art.

Applicants thus respectfully request that the claim rejections under 35 U.S.C. § 103 be withdrawn.

CONCLUSION

Applicants believe that this application is now in full condition for allowance, which action is respectfully requested. Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

Date: September 30, 2008

/Gregory A. Nelson/
Gregory A. Nelson, Registration No. 30,577
Yonghong Chen, Registration No. 56,150
AKERMAN SENTERFITT
Customer No. 40987
Post Office Box 3188
West Palm Beach, FL 33402-3188
Telephone: (561) 653-5000